3GPP TSG–SA3 Meeting #28
Berlin, Germany, 06-09 May 2003

Tdoc ⌘S3-030221

CR-Form-v7

CHANGE REQUEST

⌘	**ab.cde**	**CR**	**CRNum**	⌘**rev**	**-**	⌘	Current version:	**0.1.0**	⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects:	UICC apps⌘	☒	ME	☒	Radio Access Network	☐	Core Network	☐

Title:	⌘	Further information related to the UE's public/private key pair associated to the requested subscriber certificate.			
Source:	⌘	Gemplus			
Work item code:	⌘	Support for Subscriber Certificates	***Date:***	⌘	29/04/2003
Category:	⌘	**F**	***Release:***	⌘	Rel-6
		Use <u>one</u> of the following categories: ***F*** *(correction)* ***A*** *(corresponds to a correction in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.			*Use <u>one</u> of the following releases:* *2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)*

Reason for change:	⌘	The issuance of a valid certificate that will allow the subscriber to perform digital signatures mandates some security requirements on the public/private key pair associated to the requested certificate, since the private key pair has to be kept secret. It requires that the subscriber private key and the related cryptographic computations shall be managed by the smart cards. Those principles were already discussed in 3GPP S3-020625 contribution (Gemplus, November 2002) and agreed at Oxford SA3#26 meeting. The UICC on board key generation guaranties that nobody can access the private key.
Summary of change:	⌘	Provides further information related to the UE's public/private key pair associated to the requested subscriber certificate.
Consequences if not approved:	⌘	The privacy of the subscriber private key is not guaranted. So, there is no assurance that the issued subscriber certificate will be valid and that the digital signatures will be non-repudiable.

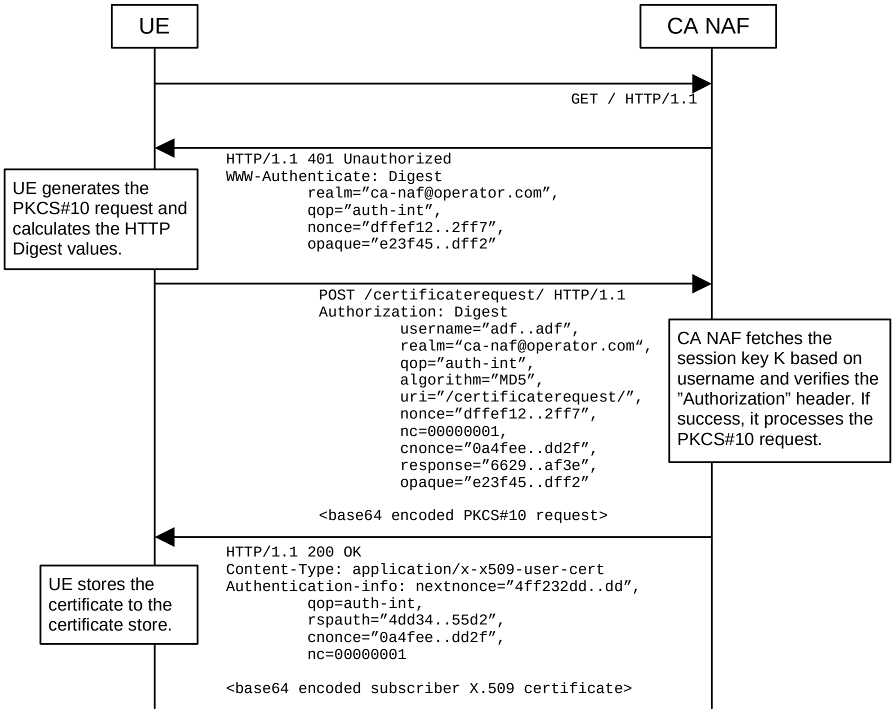
Clauses affected:	⌘	Annex A.4.1				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

A.4 Certificate issuing procedures

A.4.1 Certificate issuing

Editor's note: From five alternatives investigated in S3-030073 and S3-030036, only the following two have been agreed to add to the present document as potential solutions.

A.4.1.1 Certificate issuing using PKCS#10 with HTTP Digest Authentication


UE
CA NAF
UE generates the PKCS#10 request and calculates the HTTP Digest values.
CA NAF fetches the session key K based on username and verifies the "Authorization" header. If success, it processes the PKCS#10 request.
UE stores the certificate to the certificate store.

```
GET / HTTP/1.1
```

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Digest
         realm="ca-naf@operator.com",
         qop="auth-int",
         nonce="dffef12..2ff7",
         opaque="e23f45..dff2"
```

```
POST /certificaterequest/ HTTP/1.1
Authorization: Digest
         username="adf..adf",
         realm="ca-naf@operator.com",
         qop="auth-int",
         algorithm="MD5",
         uri="/certificaterequest/",
         nonce="dffef12..2ff7",
         nc=00000001,
         cnonce="0a4fee..dd2f",
         response="6629..af3e",
         opaque="e23f45..dff2"

<base64 encoded PKCS#10 request>
```

```
HTTP/1.1 200 OK
Content-Type: application/x-x509-user-cert
Authentication-info: nextnonce="4ff232dd..dd",
         qop=auth-int,
         rspauth="4dd34..55d2",
         cnonce="0a4fee..dd2f",
         nc=00000001

<base64 encoded subscriber X.509 certificate>
```

Figure 1: Certificate request using PKCS#10 with HTTP Digest Authentication.

The sequence diagram above describes the certificate request when using PKCS#10 with HTTP Digest. The related public/private key pair is stored in the UICC.

The sequence starts with an empty HTTP request to CA NAF. The CA NAF responds with HTTP response code 401 "Unauthorized" which contains a WWW-Authenticate header. The header instructs the UE to use HTTP Digest authentication.

The UE generates a PKCS#10 request with the subject name, public key, additional attributes and extensions. Then it will generate the HTTP request by calculating the Authorization header values using the identifier it received from the BSF as username and the session key K.

When CA NAF receives the request, it will verify the Authorization header by fetching the session key K from the bootstrapping server using the identifier, then calculating the corresponding digest values using K, and finally comparing the calculated values with the received values in the Authorization header. If the verification succeeds, the incoming PKCS#10 request is taken in for further processing. If the CA NAF is actually a registration authority (RA NAF), the PKCS#10 request is forwarded to CA using any protocol available (e.g., CMC or CMP). After the PKCS#10 request has been processed and a certificate has been created, the new certificate is returned to the CA NAF. It will generate a HTTP response containing the certificate. The CA NAF may use session key K to integrity protect and authenticate the response.

When UE receives the subscriber certificate, it is stored to local certificate management system.

A.4.1.2 Certificate issuing with CMP

CMP defines two methods to do the certificate issuing: basic authenticated scheme and centralized scheme. In the basic authenticated scheme the key generation happens in the UE while in the centralized scheme the key generation is done in the CA (or RA). CMP states that the support for the basic authenticated scheme for certificate issuing is mandatory for CAs while the support for the centralized scheme is optional. See more details in chapters 2.2 and B8 of [RFC2510].

The messages can be transported using various methods such as file based protocol, (such files can be used to transport PKI messages e.g. using FTP, HTTP, email etc.), direct TCP-based management protocol, management protocol via e-mail, and management protocol via HTTP mentioned in section 5 of [RFC2510].

A.4.1.2.1 Basic authenticated scheme

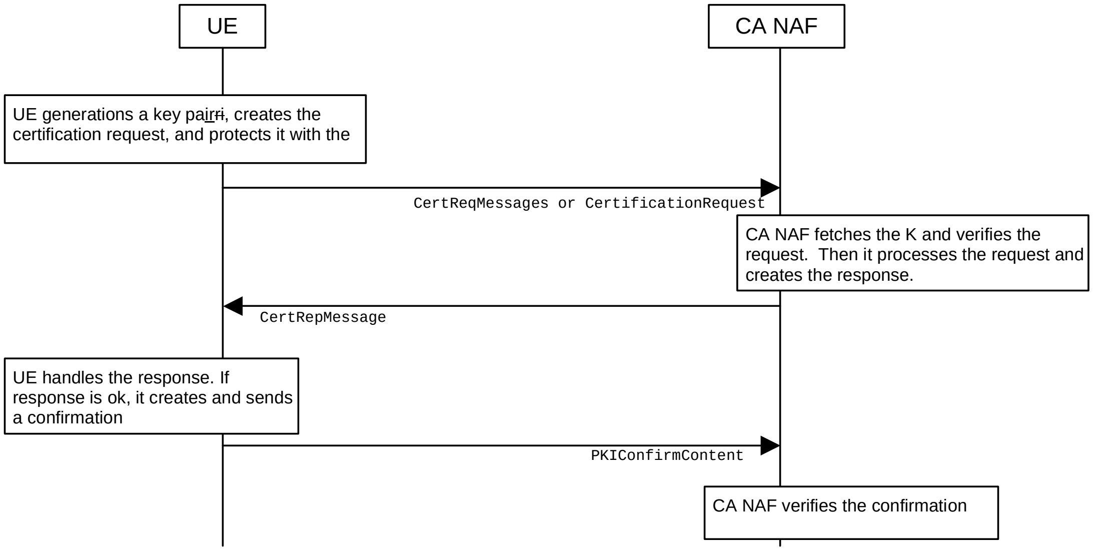

UE
CA NAF
UE generations a key pair~~ri~~, creates the certification request, and protects it with the
CertReqMessages or CertificationRequest
CA NAF fetches the K and verifies the request. Then it processes the request and creates the response.
CertRepMessage
UE handles the response. If response is ok, it creates and sends a confirmation
PKIConfirmContent
CA NAF verifies the confirmation

Figure 2: Certificate request using basic authentication scheme of CMP.

The sequence diagram above describes the certificate request and delivery procedure when using CMP and basic authenticated scheme [RFC2510]. The sequence starts with UE generating a key pair by means of UICC on board key generation, creating the certificate request message format (CRMF) message, inserting it to CertReqMessages message, and integrity protecting this message with the initial authentication key (IAK). The session key K, which has been derived earlier using protocol A, can be used as IAK.

The certificate request message is sent to CA NAF who fetches the corresponding K based on the identifier received in the request. CA NAF verifies the request with the K. If the verification succeeds, the CA NAF processes the request, i.e. generates and signs the certificate and sends the certification response to the UE.

UE verifies the certificate response message with the K. If the message verification is successful, the issued certificate is stored to the device, and UE sends a confirmation message to the CA NAF.

CA NAF verifies the confirmation message. If the verification fails or CA NAF never receives the confirmation message, CA NAF must revoke the newly issued certificate if it has been already published.

A UICC on board key generation is already defined in the WIM specification [WIM] issued by Open Mobile Alliance (OMA) group.

A.4.1.2.2 Centralized scheme initiated by the UE

The centralized scheme provides a mechanism where the public/private key pair is generated outside the UE, e.g. by the CA.

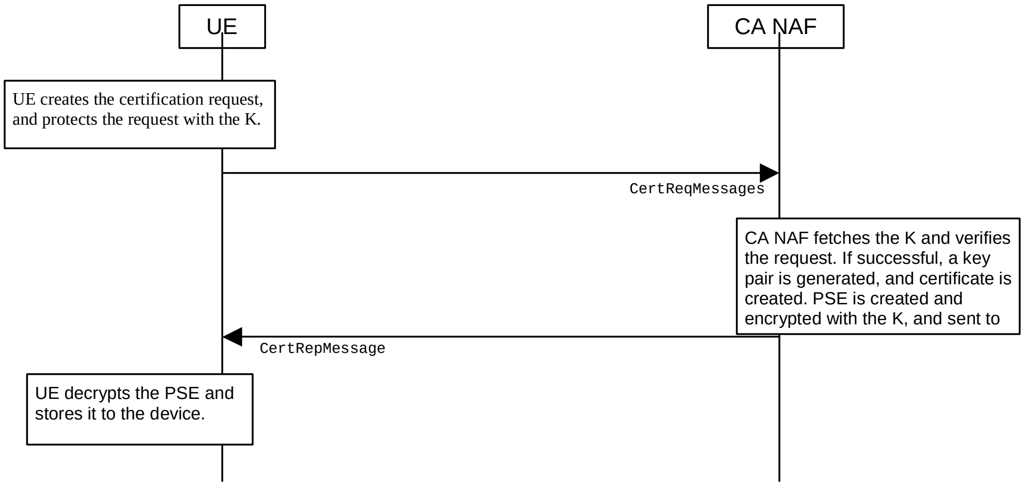

UE
CA NAF
UE creates the certification request, and protects the request with the K.
CertReqMessages
CA NAF fetches the K and verifies the request. If successful, a key pair is generated, and certificate is created. PSE is created and encrypted with the K, and sent to
CertRepMessage
UE decrypts the PSE and stores it to the device.

Figure 3: Certificate request using centralized scheme of CMP.

The sequence diagram above describes the delivery mechanism initiated by the UE using CMP in centralized scheme. This scheme is optional in CMP [RFC2510]. The sequence starts with the UE by creating CertReqMessages message with certain parameters, and protecting this message with initial authentication key (IAK). The session key K, which has been derived earlier using protocol A, can be used as IAK.

The certificate request message is sent to CA NAF who fetches the corresponding K based on the identifier received in the request. CA NAF verifies the request with the K. If the verification succeeds, CA NAF processes the request, i.e. generates a key pair, generates and signs the certificate, and sends the certification response containing the Personal Security Environment (PSE) encrypted to the UE. PSE typically contains the generated private key and newly issued certificate with corresponding public key.

UE verifies the certificate response message with the K. If the message verification is successful, the issued PSE is decrypted and stored to the device. A confirmation message is not sent in the centralized scheme.